Department of Transportation

Office of the Secretary of Transportation

49 CFR Subtitle A

■ For the reasons stated in the preamble, the Department of Transportation amends subtitle A of title 49, Code of Federal Regulations, by adding a new part 15 to read as follows:

PART 15—PROTECTION OF SENSITIVE SECURITY INFORMATION

Sec.

Authority: 49 U.S.C. 40119.

§ 15.1 Scope.

(a) *Applicability.* This part governs the maintenance, safeguarding, and disclosure of records and information that the Secretary of DOT has determined to be Sensitive Security Information, as defined in § 15.5. This part does not apply to the maintenance, safeguarding, or disclosure of classified national security information, as defined by Executive Order 12968, or to other sensitive unclassified information that is not SSI, but that nonetheless may be exempt from public disclosure under the Freedom of Information Act. In addition, in the case of information that has been designated as critical infrastructure information under section 214 of the Homeland Security Act, the receipt, maintenance, or disclosure of such information by a Federal agency or employee is governed by section 214 and any implementing regulations, not by this part.

(b) *Delegation.* The authority of the Secretary under this part may be further delegated within DOT.

§ 15.3 Terms used in this part.

In addition to the terms in § 15.3 of this chapter, the following terms apply in this part:

Administrator means the Under Secretary of Transportation for Security referred to in 49 U.S.C. 114(b), or his or her designee.

Coast Guard means the United States Coast Guard.

Covered person means any organization, entity, individual, or other person described in § 15.7. In the case of an individual, *covered person* includes any individual applying for employment in a position that would be a covered person, or in training for such a position, regardless of whether that individual is receiving a wage, salary, or other form of payment. *Covered person* includes a person applying for certification or other form of approval that, if granted, would make the person a covered person described in § 15.7.

DHS means the Department of Homeland Security and any directorate, bureau, or other component within the Department of Homeland Security, including the United States Coast Guard.

DOT means the Department of Transportation and any operating administration, entity, or office within the Department of Transportation, including the Saint Lawrence Seaway Development Corporation and the Bureau of Transportation Statistics.

Federal Flight Deck Officer means a pilot participating in the Federal Flight Deck Officer Program under 49 U.S.C. 44921 and implementing regulations.

Maritime facility means any facility as defined in 33 CFR part 101.

Record includes any means by which information is preserved, irrespective of format, including a book, paper, drawing, map, recording, tape, film, photograph, machine-readable material, and any information stored in an electronic format. The term *record* also includes any draft, proposed, or recommended change to any record.

Security contingency plan means a plan detailing response procedures to address a transportation security incident, threat assessment, or specific threat against transportation, including details of preparation, response, mitigation, recovery, and reconstitution procedures, continuity of government, continuity of transportation operations, and crisis management.

Security program means a program or plan and any amendments developed for the security of the following, including any comments, instructions, or implementing guidance:

(1) An airport, aircraft, or aviation cargo operation;

(2) A maritime facility, vessel, or port area; or

(3) A transportation-related automated system or network for information processing, control, and communications.

Security screening means evaluating a person or property to determine whether either poses a threat to security.

SSI means sensitive security information, as described in § 15.5.

Threat image projection system means an evaluation tool that involves periodic presentation of fictional threat images to operators and is used in connection with x-ray or explosives detection systems equipment.

TSA means the Transportation Security Administration.

Vulnerability assessment means any review, audit, or other examination of the security of a transportation infrastructure asset; airport; maritime facility, port area, vessel, aircraft, train, commercial motor vehicle, or pipeline, or a transportation-related automated system or network, to determine its vulnerability to unlawful interference, whether during the conception, planning, design, construction, operation, or decommissioning phase. A *vulnerability assessment* may include proposed, recommended, or directed actions or countermeasures to address security concerns.

§ 15.5 Sensitive security information.

(a) *In general.* In accordance with 49 U.S.C. 40119(b)(1), SSI is information obtained or developed in the conduct of security activities, including research and development, the disclosure of which the Secretary of DOT has determined would—

(1) Constitute an unwarranted invasion of privacy (including, but not limited to, information contained in any personnel, medical, or similar file);

(2) Reveal trade secrets or privileged or confidential information obtained from any person; or

(3) Be detrimental to transportation safety.

(b) *Information constituting SSI.* Except as otherwise provided in writing by the Secretary of DOT in the interest of public safety or in furtherance of transportation security, the following information, and records containing such information, constitute SSI:

(1) *Security programs and contingency plans.* Any security program or security contingency plan issued, established, required, received, or approved by DOT or DHS, including—

(i) Any aircraft operator or airport operator security program or security contingency plan under this chapter;

(ii) Any vessel, maritime facility, or port area security plan required or directed under Federal law;

(iii) Any national or area security plan prepared under 46 U.S.C. 70103; and

(iv) Any security incident response plan established under 46 U.S.C. 70104.

(2) *Security Directives.* Any Security Directive or order—

(i) Issued by TSA under 49 CFR 1542.303, 1544.305, or other authority;

(ii) Issued by the Coast Guard under the Maritime Transportation Security Act, 33 CFR part 6, or 33 U.S.C. 1221 *et seq.* related to maritime security; or

(iii) Any comments, instructions, and implementing guidance pertaining thereto.

(3) *Information Circulars.* Any notice issued by DHS or DOT regarding a threat to aviation or maritime transportation, including any—

(i) Information Circular issued by TSA under 49 CFR 1542.303 or 1544.305, or other authority; and

(ii) Navigation or Vessel Inspection Circular issued by the Coast Guard related to maritime security.

(4) *Performance specifications.* Any performance specification and any description of a test object or test procedure, for—

(i) Any device used by the Federal government or any other person pursuant to any aviation or maritime transportation security requirements of Federal law for the detection of any weapon, explosive, incendiary, or destructive device or substance; and

(ii) Any communications equipment used by the Federal government or any other person in carrying out or complying with any aviation or maritime transportation security requirements of Federal law.

(5) *Vulnerability assessments.* Any vulnerability assessment directed, created, held, funded, or approved by the DOT, DHS, or that will be provided to DOT or DHS in support of a Federal security program.

(6) *Security inspection or investigative information.* (i) Details of any security inspection or investigation of an alleged violation of aviation or maritime transportation security requirements of Federal law that could reveal a security vulnerability, including the identity of the Federal special agent or other Federal employee who conducted the inspection or audit.

(ii) In the case of inspections or investigations performed by TSA, this includes the following information as to events that occurred within 12 months of the date of release of the information: the name of the airport where a violation occurred, the airport identifier in the case number, a description of the violation, the regulation allegedly violated, and the identity of any aircraft operator in connection with specific locations or specific security procedures. Such information will be released after the relevant 12-month period, except that TSA will not release the specific gate or other location on an airport where an event occurred, regardless of the amount of time that has passed since its occurrence. During the period within 12 months of the date of release of the information, TSA may release summaries of an aircraft operator's, but not an airport operator's, total security violations in a specified time range without identifying specific violations or locations. Summaries may include total enforcement actions, total proposed civil penalty amounts, number of cases opened, number of cases referred to TSA or FAA counsel for legal enforcement action, and number of cases closed.

(7) *Threat information.* Any information held by the Federal government concerning threats against transportation or transportation systems and sources and methods used to gather or develop threat information, including threats against cyber infrastructure.

(8) *Security measures.* Specific details of aviation or maritime transportation security measures, both operational and technical, whether applied directly by the Federal government or another person, including—

(i) Security measures or protocols recommended by the Federal government;

(ii) Information concerning the deployments, numbers, and operations of Coast Guard personnel engaged in maritime security duties and Federal Air Marshals, to the extent it is not classified national security information; and

(iii) Information concerning the deployments and operations of Federal Flight Deck Officers, and numbers of Federal Flight Deck Officers aggregated by aircraft operator.

(9) *Security screening information.* The following information regarding security screening under aviation or maritime transportation security requirements of Federal law:

(i) Any procedures, including selection criteria and any comments, instructions, and implementing guidance pertaining thereto, for screening of persons, accessible property, checked baggage, U.S. mail, stores, and cargo, that is conducted by the Federal government or any other authorized person.

(ii) Information and sources of information used by a passenger or property screening program or system, including an automated screening system.

(iii) Detailed information about the locations at which particular screening methods or equipment are used, only if determined by TSA to be SSI.

(iv) Any security screener test and scores of such tests.

(v) Performance or testing data from security equipment or screening systems.

(vi) Any electronic image shown on any screening equipment monitor, including threat images and descriptions of threat images for threat image projection systems.

(10) *Security training materials.* Records created or obtained for the purpose of training persons employed by, contracted with, or acting for the Federal government or another person to carry out any aviation or maritime transportation security measures required or recommended by DHS or DOT.

(11) *Identifying information of certain transportation security personnel.* (i) Lists of the names or other identifying information that identify persons as—

(A) Having unescorted access to a secure area of an airport or a secure or restricted area of a maritime facility, port area, or vessel or;

(B) Holding a position as a security screener employed by or under contract with the Federal government pursuant to aviation or maritime transportation security requirements of Federal law, where such lists are aggregated by airport;

(C) Holding a position with the Coast Guard responsible for conducting vulnerability assessments, security boardings, or engaged in operations to enforce maritime security requirements or conduct force protection;

(D) Holding a position as a Federal Air Marshal; or

(ii) The name or other identifying information that identifies a person as a current, former, or applicant for Federal Flight Deck Officer.

(12) *Critical aviation or maritime infrastructure asset information.* Any list identifying systems or assets, whether physical or virtual, so vital to the aviation or maritime transportation system that the incapacity or destruction of such assets would have a debilitating impact on transportation security, if the list is—

(i) Prepared by DHS or DOT; or

(ii) Prepared by a State or local government agency and submitted by the agency to DHS or DOT.

(13) *Systems security information.* Any information involving the security of operational or administrative data systems operated by the Federal government that have been identified by the DOT or DHS as critical to aviation or maritime transportation safety or security, including automated information security procedures and systems, security inspections, and vulnerability information concerning those systems.

(14) *Confidential business information.* (i) Solicited or unsolicited proposals received by DHS or DOT, and negotiations arising therefrom, to perform work pursuant to a grant, contract, cooperative agreement, or other transaction, but only to the extent that the subject matter of the proposal relates to aviation or maritime transportation security measures;

(ii) Trade secret information, including information required or requested by regulation or Security Directive, obtained by DHS or DOT in carrying out aviation or maritime transportation security responsibilities; and

(iii) Commercial or financial information, including information required or requested by regulation or Security Directive, obtained by DHS or DOT in carrying out aviation or maritime transportation security responsibilities, but only if the source of the information does not customarily disclose it to the public.

(15) *Research and development.* Information obtained or developed in the conduct of research related to aviation or maritime transportation security activities, where such research is approved, accepted, funded, recommended, or directed by the DHS or DOT, including research results.

(16) *Other information.* Any information not otherwise described in this section that TSA determines is SSI under 49 U.S.C. 114(s) or that the Secretary of DOT determines is SSI under 49 U.S.C. 40119. Upon the request of another Federal agency, the Secretary of DOT may designate as SSI information not otherwise described in this section.

(c) *Loss of SSI designation.* The Secretary of DOT may determine in writing that information or records described in paragraph (b) of this section do not constitute SSI because they no longer meet the criteria set forth in paragraph (a) of this section.

§ 15.7 Covered persons.

Persons subject to the requirements of part 15 are:

(a) Each airport operator and aircraft operator subject to the requirements of Subchapter C of this title.

(b) Each indirect air carrier, as defined in 49 CFR 1540.5.

(c) Each owner, charterer, or operator of a vessel, including foreign vessel owners, charterers, and operators, required to have a security plan under Federal or International law.

(d) Each owner or operator of a maritime facility required to have a security plan under the Maritime Transportation Security Act, (Pub. L. 107–295), 46 U.S.C. 70101 *et seq.*, 33 CFR part 6, or 33 U.S.C. 1221 *et seq.*

(e) Each person performing the function of a computer reservation system or global distribution system for airline passenger information.

(f) Each person participating in a national or area security committee established under 46 U.S.C. 70112, or a port security committee.

(g) Each industry trade association that represents covered persons and has entered into a non-disclosure agreement with the DHS or DOT.

(h) DHS and DOT.

(i) Each person conducting research and development activities that relate to aviation or maritime transportation security and are approved, accepted, funded, recommended, or directed by DHS or DOT.

(j) Each person who has access to SSI, as specified in § 15.11.

(k) Each person employed by, contracted to, or acting for a covered person, including a grantee of DHS or DOT, and including a person formerly in such position.

(l) Each person for which a vulnerability assessment has been directed, created, held, funded, or approved by the DOT, DHS, or that has prepared a vulnerability assessment that will be provided to DOT or DHS in support of a Federal security program.

(m) Each person receiving SSI under § 1520.15(d) or (e).

§ 15.9 Restrictions on the disclosure of SSI.

(a) *Duty to protect information.* A covered person must—

(1) Take reasonable steps to safeguard SSI in that person's possession or control from unauthorized disclosure. When a person is not in physical possession of SSI, the person must store it a secure container, such as a locked desk or file cabinet or in a locked room.

(2) Disclose, or otherwise provide access to, SSI only to covered persons who have a need to know, unless otherwise authorized in writing by TSA, the Coast Guard, or the Secretary of DOT.

(3) Refer requests by other persons for SSI to TSA or the applicable component or agency within DOT or DHS.

(4) Mark SSI as specified in § 15.13.

(5) Dispose of SSI as specified in § 15.19.

(b) *Unmarked SSI.* If a covered person receives a record containing SSI that is not marked as specified in § 1520.13, the covered person must—

(1) Mark the record as specified in § 15.13; and

(2) Inform the sender of the record that the record must be marked as specified in § 15.13.

(c) *Duty to report unauthorized disclosure.* When a covered person

becomes aware that SSI has been released to unauthorized persons, the covered person must promptly inform TSA or the applicable DOT or DHS component or agency.

(d) *Additional requirements for critical infrastructure information.* In the case of information that is both SSI and has been designated as critical infrastructure information under section 214 of the Homeland Security Act, any covered person who is a Federal employee in possession of such information must comply with the disclosure restrictions and other requirements applicable to such information under section 214 and any implementing regulations.

§ 15.11 Persons with a need to know.

(a) *In general.* A person has a need to know SSI in each of the following circumstances:

(1) When the person requires access to specific SSI to carry out aviation or maritime transportation security activities approved, accepted, funded, recommended, or directed by DHS or DOT.

(2) When the person is in training to carry out aviation or maritime transportation security activities approved, accepted, funded, recommended, or directed by DHS or DOT.

(3) When the information is necessary for the person to supervise or otherwise manage individuals carrying out aviation or maritime transportation security activities approved, accepted, funded, recommended, or directed by the DHS or DOT.

(4) When the person needs the information to provide technical or legal advice to a covered person regarding aviation or maritime transportation security requirements of Federal law.

(5) When the person needs the information to represent a covered person in connection with any judicial or administrative proceeding regarding those requirements.

(b) *Federal employees, contractors, and grantees.* (1) A Federal employee has a need to know SSI if access to the information is necessary for performance of the employee's official duties.

(2) A person acting in the performance of a contract with or grant from DHS or DOT has a need to know SSI if access to the information is necessary to performance of the contract or grant.

(c) *Background check.* The Secretary of DOT may make an individual's access to the SSI contingent upon satisfactory completion of a security background check and the imposition of procedures and requirements for safeguarding SSI that are satisfactory to the Secretary.

(d) *Need to know further limited by the DHS or DOT.* For some specific SSI, DHS or DOT may make a finding that only specific persons or classes of persons have a need to know.

§ 15.13 Marking SSI.

(a) *Marking of paper records.* In the case of paper records containing SSI, a covered person must mark the record by placing the protective marking conspicuously on the top, and the distribution limitation statement on the bottom, of—

(1) The outside of any front and back cover, including a binder cover or folder, if the document has a front and back cover;

(2) Any title page; and

(3) Each page of the document.

(b) *Protective marking.* The protective marking is: SENSITIVE SECURITY INFORMATION.

(c) *Distribution limitation statement.* The distribution limitation statement is:

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a ''need to know'', as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

(d) *Other types of records.* In the case of non-paper records that contain SSI, including motion picture films, videotape recordings, audio recording, and electronic and magnetic records, a covered person must clearly and conspicuously mark the records with the protective marking and the distribution limitation statement such that the viewer or listener is reasonably likely to see or hear them when obtaining access to the contents of the record.

§ 15.15 SSI disclosed by DOT.

(a) *In general.* Except as otherwise provided in this section, and notwithstanding the Freedom of Information Act (5 U.S.C. 552), the Privacy Act (5 U.S.C. 552a), and other laws, records containing SSI are not available for public inspection or copying, nor does DOT release such records to persons without a need to know.

(b) *Disclosure under the Freedom of Information Act and the Privacy Act.* If a record contains both SSI and information that is not SSI, DOT, on a proper Freedom of Information Act or Privacy Act request, may disclose the record with the SSI redacted, provided the record is not otherwise exempt from disclosure under the Freedom of Information Act or Privacy Act.

(c) *Disclosures to committees of Congress and the General Accounting Office.* Nothing in this part precludes DOT from disclosing SSI to a committee of Congress authorized to have the information or to the Comptroller General, or to any authorized representative of the Comptroller General.

(d) *Disclosure in enforcement proceedings.* (1) *In general.* The Secretary of DOT may provide SSI to a person in the context of an administrative enforcement proceeding when, in the sole discretion of the Secretary, access to the SSI is necessary for the person to prepare a response to allegations contained in a legal enforcement action document issued by DOT.

(2) *Security background check.* Prior to providing SSI to a person under paragraph (d)(1) of this section, the Secretary of DOT may require the individual or, in the case of an entity, the individuals representing the entity, and their counsel, to undergo and satisfy, in the judgment of the Secretary of DOT, a security background check.

(e) *Other conditional disclosure.* The Secretary of DOT may authorize a conditional disclosure of specific records or information that constitute SSI upon the written determination by the Secretary that disclosure of such records or information, subject to such limitations and restrictions as the Secretary may prescribe, would not be detrimental to transportation safety.

(f) *Obligation to protect information.* When an individual receives SSI pursuant to paragraph (d) or (e) of this section that individual becomes a covered person under § 15.7 and is subject to the obligations of a covered person under this part.

(g) *No release under FOIA.* When DOT discloses SSI pursuant to paragraphs (b) through (e) of this section, DOT makes the disclosure for the sole purpose described in that paragraph. Such disclosure is not a public release of information under the Freedom of Information Act.

(h) *Disclosure of Critical Infrastructure Information.* Disclosure of information that is both SSI and has been designated as critical infrastructure information under section 214 of the Homeland Security Act is governed solely by the requirements of section 214 and any implementing regulations.

§ 15.17 Consequences of unauthorized disclosure of SSI.

Violation of this part is grounds for a civil penalty and other enforcement or corrective action by DOT, and appropriate personnel actions for Federal employees. Corrective action may include issuance of an order requiring retrieval of SSI to remedy unauthorized disclosure or an order to cease future unauthorized disclosure.

§ 15.19 Destruction of SSI.

(a) *DOT.* Subject to the requirements of the Federal Records Act (5 U.S.C. 105), including the duty to preserve records containing documentation of a Federal agency's policies, decisions, and essential transactions, DOT destroys SSI when no longer needed to carry out the agency's function.

(b) *Other covered persons.* (1) *In general.* A covered person must destroy SSI completely to preclude recognition or reconstruction of the information when the covered person no longer needs the SSI to carry out transportation security measures.

(2) *Exception.* Paragraph (b)(1) of this section does not require a State or local government agency to destroy information that the agency is required to preserve under State or local law.

Issued in Washington, DC, on May 6, 2004.

Norman Y. Mineta,

Secretary of Transportation.